(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0079191
(43) 공개일자 2020년07월02일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/16* (2006.01)
(52) CPC특허분류
H04L 9/321 (2013.01)
H04L 9/16 (2013.01)
(21) 출원번호 10-2019-0167819
(22) 출원일자 2019년12월16일
심사청구일자 2019년12월16일
(30) 우선권주장
1020180168456 2018년12월24일 대한민국(KR)
기술이전 희망 : 기술양도

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 아카데미로 119 (송도동)
(72) 발명자
이은규
인천광역시 연수구 해돋이로120번길 16, 213동 1002호(송도동, 송도풍림아이원2단지아파트)
(74) 대리인
특허법인충정

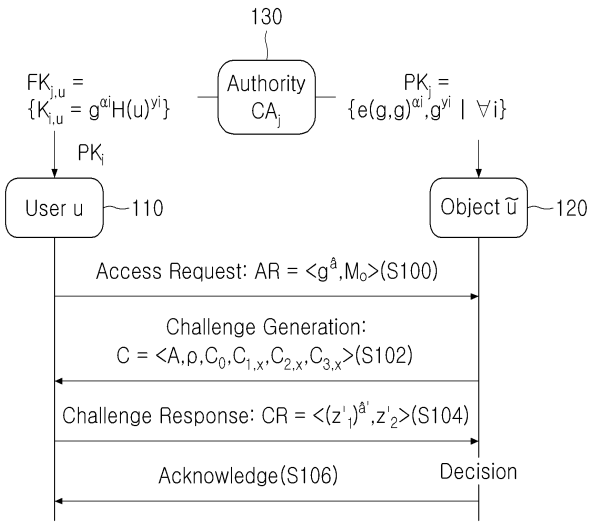
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **우선 순위가 설정된 멀티 팩터 액세스 제어 시스템 및 방법**

(57) 요 약

우선 순위가 설정된 멀티 팩터 액세스 제어 시스템 및 방법은 우선 순위 지정 문제를 해결하기 위하여 우선 순위가 높은 객체에 액세스할 때, 서로 독립적인 복수의 인증기관으로부터 2가지 이상의 팩터 키를 제공받으며, 팩터 키의 개수를 조정하여 사용자의 보호 수준을 동적으로 변경할 수 있다.

대 표 도 - 도3



(52) CPC특허분류
H04L 9/3271 (2013.01)
H04L 2463/082 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 201601750003
부처명 과학기술정보통신부
연구관리전문기관 한국연구재단
연구사업명 신진연구지원사업
연구과제명 차세대 IoT 서비스 실현을 위한 엣지 컴퓨팅과 데이터 네트워킹 기반의 엣지 네트워크 시스템 개발에 관한 연구
기 여 율 1/1
주관기관 인천대학교 산학협력단
연구기간 2016.06.01 ~ 2019.05.31

명 세 서

청구범위

청구항 1

유무선 네트워크를 통하여 인증기관, 사용자 단말과 서비스 제공 단말 간의 액세스 제어를 수행하는 멀티 팩터 액세스 제어 방법에 있어서,

상기 인증기관은 하나 이상으로 형성되고, 상기 각각의 인증기관로부터 액세스 제어를 위한 팩터(Factor) 키를 하나 이상을 생성하여 상기 사용자 단말과 상기 서비스 제공 단말로 전송하는 단계;

상기 사용자 단말은 상기 인증기관으로부터 수신한 팩터 키와 본인을 나타내는 랜덤번호를 포함한 상기 서비스 제공 단말의 액세스 제어를 위한 액세스 요청 메시지를 생성하여 상기 서비스 제공 단말로 전송하는 단계;

상기 서비스 제공 단말은 상기 사용자 단말로부터 상기 액세스 요청 메시지를 수신하는 경우, 상기 사용자 단말이 가진 속성으로 구성된 액세스 정책 트리를 수학적으로 암호화하는 챌린지(C)를 생성하고, 상기 생성한 챌린지(C)를 상기 사용자 단말로 전송하는 단계;

상기 사용자 단말은 상기 랜덤번호를 이용하여 상기 챌린지(C)에 대응하는 챌린지 응답 신호를 생성하고, 상기 생성한 챌린지 응답 신호를 상기 서비스 제공 단말로 전송하는 단계; 및

상기 서비스 제공 단말은 상기 챌린지 응답 신호를 수신하고, 상기 수신한 챌린지 응답 신호에 포함된 고유 시퀀스 번호와, 상기 고유 시퀀스 번호를 이용하여 복호화 연산 과정을 수행한 결과값을 비교하여 액세스 성공 여부를 판단하는 단계를 포함하는 것을 특징으로 하는 멀티 팩터 액세스 제어 방법.

청구항 2

제1항에 있어서,

상기 사용자 단말은 본인을 나타내는 랜덤번호인 $\hat{a} \in \mathbb{Z}$를 생성하고, 하기의 수학식 1과 같이, $g^{\hat{a}}$를 포함한 액세스 요청 메시지(Mo)를 생성하여 상기 서비스 제공 단말로 전송하는 단계를 포함하는 것을 특징으로 하는 멀티 팩터 액세스 제어 방법.

[수학식 1]

$$u \mapsto \tilde{u} : \mathcal{AR} = \langle g^{\hat{a}}, M_o \rangle$$

청구항 3

제2항에 있어서,

상기 서비스 제공 단말은 2개의 랜덤번호인 $\hat{b}$ and $\hat{c} \in \mathbb{Z}$를 생성하고, 시퀀스 번호 z를 생성하고, 상기 액세스 요청 메시지에서 획득한 상기 $g^{\hat{a}}$를 이용하여 2개의 변수(Z_1, Z_2)를 수학식 2에 의해 계산하고, 상기 2개의 변수를 연결하여 수학식 3의 챌린지 메시지(Mc)를 생성하며, 상기 생성한 챌린지 메시지를 상기 사용자 단말로 전송하는 단계를 포함하는 것을 특징으로 하는 멀티 팩터 액세스 제어 방법.

[수학식 2]

$$z_1 = g^{\hat{b}} \text{ and } z_2 = enc_z(\hat{c}, (g^{\hat{a}})^{\hat{b}\hat{c}})$$

여기서, $enc_x(y)$는 메시지 y를 팩터 x로 암호화하는 대칭 키 알고리즘임.

[수학식 3]

$$M_c = \langle z_1, z_2 \rangle$$

여기서, $<Z_1, Z_2>$는 Z_1와 Z_2를 연결함.

청구항 4

제3항에 있어서,

상기 사용자 단말은 액세스 요청 절차에서 미리 선택된 랜덤번호 $\hat{a} \in \mathbb{Z}$를 이용하여 하기의 수학식 4와 같은 챌린지 응답 신호(CR)를 생성하고, 상기 생성한 챌린지 응답 신호를 상기 서비스 제공 단말로 전송하고,

상기 서비스 제공 단말은 상기 사용자 단말로부터 챌린지 응답 신호를 수신하는 경우, z_2'를 획득하고, 챌린지 생성 절차에서 사용된 고유 시퀀스 번호 Z를 사용하여 $dec_z(z_2') = \langle \hat{c}, (g^{\hat{a}})^{\hat{b}\hat{c}} \rangle$의 복호화 연산 과정을 계산하고, 하기의 수학식 5와 같이 2개의 변수를 비교한 후, 비교 결과가 동일하면, True를 반환하는 경우, 상기 액세스 요청 메시지에 따라 액세스 요청을 수행하며, 비교 결과가 동일하지 않으면, False를 반환하는 경우, 상기 액세스 요청 메시지에 따라 액세스 요청을 거부하는 단계를 포함하는 것을 특징으로 하는 멀티 팩터 액세스 제어 방법.

[수학식 4]

$$u \mapsto \tilde{u} : \mathcal{CR} = \langle (z_1')^{\hat{a}'}, z_2' \rangle$$

[수학식 5]

$$((z_1')^{\hat{a}'})^{\hat{c}} = (g^{\hat{a}})^{\hat{b}\hat{c}}$$

청구항 5

액세스 제어를 위한 팩터(Factor) 키를 하나 이상을 생성하여 전송하는 하나 이상의 인증기관;

상기 인증기관으로부터 수신한 팩터 키와 본인을 나타내는 랜덤번호를 포함한 액세스 제어를 위한 액세스 요청 메시지를 생성하여 전송하는 사용자 단말; 및

상기 사용자 단말로부터 상기 액세스 요청 메시지를 수신하는 경우, 상기 사용자 단말이 가진 속성으로 구성된 액세스 정책 트리를 수학적으로 암호화하는 챌린지(C)를 생성하고, 상기 생성한 챌린지(C)를 상기 사용자 단말로 전송하고, 상기 사용자 단말로부터 상기 랜덤번호를 이용하여 상기 챌린지(C)에 대응하는 챌린지 응답 신호를 수신하며, 상기 수신한 챌린지 응답 신호에 포함된 고유 시퀀스 번호와, 상기 고유 시퀀스 번호를 이용하여 복호화 연산 과정을 수행한 결과값을 비교하여 액세스 성공 여부를 판단하는 서비스 제공 단말을 포함하는 것을 특징으로 하는 멀티 팩터 액세스 제어 시스템.

청구항 6

액세스 제어를 위한 팩터(Factor) 키를 하나 이상을 생성하여 전송하는 복수의 인증기관;

상기 하나의 인증기관 또는 상기 2개 이상의 인증기관으로부터 액세스 제어를 위한 팩터(Factor) 키를 수신하여 권한을 부여받는 복수의 사용자 단말; 및

상기 각각의 사용자 단말로부터 수신된 팩터 키들의 속성들에 따라 상기 각각의 사용자 단말을 인증하고, 상기 각각의 사용자 단말에서 특정 액세스 조작을 나타내는 속성으로 구성된 액세스 정책 트리를 수학적으로 암호화하여 상기 각각의 사용자 단말로 전송하는 서비스 제공 단말을 포함하며,

상기 서비스 제공 단말은 일정 시간 후에 상기 액세스 정책 트리의 구조를 동적으로 변경하여 팩터별로 보호 수준의 난이도를 다르게 설정하는 것을 특징으로 하는 멀티 팩터 액세스 제어 시스템.

청구항 7

제5항 또는 제6항에 있어서,

상기 사용자 단말은 본인을 나타내는 랜덤번호인 $\hat{a} \in \mathbb{Z}$를 생성하고, 하기의 수학식 1과 같이, $g^{\hat{a}}$를 포함한 액세스 요청 메시지(Mo)를 생성하여 상기 서비스 제공 단말로 전송하는 것을 특징으로 하는 멀티 팩터 액세스 제어 시스템.

[수학식 1]

$$u \mapsto \tilde{u} : \mathcal{AR} = \langle g^{\hat{a}}, M_o \rangle$$

청구항 8

제5항 또는 제6항에 있어서,

상기 서비스 제공 단말은 상기 팩터 키들의 속성들을 이용하여 2개의 입력과 하나의 출력을 갖는 논리 회로를 복수로 구성된 상기 액세스 정책 트리를 텍스트 형태로 나타내고, 상기 텍스트 형태를 등가의 n(액세스 정책 트리의 형태로 결정함)×l(액세스 정책 트리의 속성 개수)의 LSSS(Linear Secret Sharing Scheme) 매트릭스 형태로 변환하며, 상기 변환한 매트릭스 형태를 수학적으로 암호화하는 것을 특징으로 하는 멀티 팩터 액세스 제어 시스템.

청구항 9

제7항에 있어서,

상기 서비스 제공 단말은 2개의 랜덤번호인 $\hat{b}$ and $\hat{c} \in \mathbb{Z}$를 생성하고, 시퀀스 번호 z를 생성하고, 상기 액세스 요청 메시지에서 획득한 상기 $g^{\hat{a}}$를 이용하여 2개의 변수(Z_1, Z_2)를 수학식 2에 의해 계산하고, 상기 2개의 변수를 연결하여 수학식 3의 챌린지 메시지(Mc)를 생성하며, 상기 생성한 챌린지 메시지를 상기 사용자 단말로 전송하는 것을 특징으로 하는 멀티 팩터 액세스 제어 시스템.

[수학식 2]

$$z_1 = g^{\hat{b}} \text{ and } z_2 = enc_z(\hat{c}, (g^{\hat{a}})^{\hat{b}\hat{c}})$$

여기서, $enc_x(y)$는 메시지 y를 팩터 x로 암호화하는 대칭 키 알고리즘임.

[수학식 3]

$$M_c = \langle z_1, z_2 \rangle$$

여기서, $\langle Z_1, Z_2 \rangle$는 Z_1와 Z_2를 연결함.

청구항 10

제9항에 있어서,

상기 사용자 단말은 액세스 요청 절차에서 미리 선택된 랜덤번호 $\hat{a} \in \mathbb{Z}$를 이용하여 하기의 수학식 4와 같은 챌린지 응답 신호(CR)를 생성하고, 상기 생성한 챌린지 응답 신호를 상기 서비스 제공 단말로 전송하고,

상기 서비스 제공 단말은 상기 사용자 단말로부터 챌린지 응답 신호를 수신하는 경우, z'_2를 획득하고, 챌린지 생성 절차에서 사용된 고유 시퀀스 번호 Z를 사용하여 $dec_z(z'_2) = \langle \hat{c}, (g^{\hat{a}})^{\hat{b}\hat{c}} \rangle$의 복호화 연산 과정을 계산하고, 하기의 수학식 5와 같이 2개의 변수를 비교한 후, 비교 결과가 동일하면, True를 반환하는 경우, 상기 액세스 요청 메시지에 따라 액세스 요청을 수행하며, 비교 결과가 동일하지 않으면, False를 반환하는 경우, 상기 액세스 요청 메시지에 따라 액세스 요청을 거부하는 것을 특징으로 하는 멀티 팩터 액세스 제어 시스템.

[수학식 4]

$$u \mapsto \tilde{u} : \mathcal{CR} = \langle (z'_1)^{\hat{a}'}, z'_2 \rangle$$

[수학식 5]

$$((z'_1)^{\hat{a}'})^{\hat{c}} = (g^{\hat{a}})^{\hat{b}\hat{c}}$$

발명의 설명

기 술 분 야

[0001] 본 발명은 액세스 제어 시스템에 관한 것으로서, 특히 우선 순위 지정 문제를 해결하기 위하여 우선 순위가 높은 객체에 액세스할 때, 서로 독립적인 복수의 인증기관으로부터 2가지 이상의 팩터 키를 제공받으며, 팩터 키의 개수를 조정하여 사용자의 보호 수준을 동적으로 변경할 수 있는 우선 순위가 설정된 멀티 팩터 액세스 제어 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 사물 인터넷 환경에서는 액세스 제어를 조사하여 사용자의 요청을 허용하거나 거부하는 결정을 내린다.

[0003] 물리적 시스템에서의 액세스 작업은 인간에게 다양한 영향을 미치기 때문에 중요하다. 원자력 발전소를 제어하는 것과 데이터를 읽는 것은 우선 순위가 달라야 한다.

[0004] 이러한 인증 작업에 대한 액세스 요청은 우선 순위 지정 문제라는 여러 가지의 보호 수준으로 구분하여 인증되어야 한다.

[0005] 그러나 기존의 인증 솔루션은 우선 순위의 요구 사항을 충족시키지 못하거나 사물 인터넷 환경에서 잘 작동하지 않는 문제점이 있었다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국 등록특허번호 제10-1632946호

발명의 내용

해결하려는 과제

[0007] 이와 같은 문제점을 해결하기 위하여, 본 발명은 우선 순위 지정 문제를 해결하기 위하여 우선 순위가 높은 객체에 액세스할 때, 서로 독립적인 복수의 인증기관으로부터 2가지 이상의 팩터 키를 제공받으며, 팩터 키의 개수를 조정하여 사용자의 보호 수준을 동적으로 변경할 수 있는 우선 순위가 설정된 멀티 팩터 액세스 제어 시스템 및 방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

[0008] 상기 목적을 달성하기 위한 본 발명의 특징에 따른 우선 순위가 설정된 멀티 팩터 액세스 제어 방법은,

[0009] 유무선 네트워크를 통하여 인증기관, 사용자 단말과 서비스 제공 단말 간의 인증 프로세스를 수행하는 멀티 팩터 액세스 제어 방법에 있어서,

[0010] 상기 인증기관은 복수개로 형성되고, 상기 각각의 인증기관에서 인증 과정을 위한 팩터 키와 공개 키를 생성하고, 상기 하나 이상의 팩터 키와 공개 키를 상기 사용자 단말로 전송하는 단계;

[0011] 상기 사용자 단말은 액세스 요청 메시지를 생성하여 상기 서비스 제공 단말로 전송하는 단계;

[0012] 상기 서비스 제공 단말은 상기 사용자 단말로부터 상기 액세스 요청 메시지를 수신하는 경우, 상기 사용자 단말을 인증하는데 사용되는 챌린지 C를 생성하고, 상기 생성한 챌린지 C를 상기 사용자 단말로 전송하는 단계;

[0013] 상기 사용자 단말은 액세스 요청 절차에서 미리 선택된 임의의 수를 이용하여 상기 챌린지 C에 대응하는 챌린지 응답 신호를 생성하고, 상기 생성한 챌린지 응답 신호를 상기 서비스 제공 단말로 전송하는 단계; 및

[0014] 상기 서비스 제공 단말은 상기 챌린지 응답 신호를 수신하고, 상기 수신한 챌린지 응답 신호에 포함된 고유 시퀀스 번호와, 상기 고유 시퀀스 번호를 이용하여 복호화 연산 과정을 수행하는 단계를 포함하는 것을 특징으로 한다.

발명의 효과

[0015] 전술한 구성에 의하여, 본 발명은 서로 독립적인 복수의 인증기관으로부터 2가지 이상의 팩터 키를 제공받으며, 팩터 키의 개수를 조정하여 사용자의 보호 수준을 동적으로 변경할 수 있으므로 자체 액세스 제어 정책을 구성할 수 있는 효과가 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 실시예에 따른 우선 순위가 설정된 멀티 팩터 액세스 제어 시스템의 구성을 나타낸 도면이다.

도 2는 본 발명의 실시예에 따른 액세스 정책 트리의 일례를 나타낸 도면이다.

도 3은 본 발명의 실시예에 따른 멀티 팩터 액세스 제어 시스템에서 인증 및 권한 부여 프로토콜의 액세스 제어 결정을 위한 프로토콜을 나타낸 도면이다.

도 4는 본 발명의 실시예에 따른 스마트 그리드의 멀티 팩터 액세스 제어를 사용하여 에너지 자원에 대한 세분화된 액세스 제어 개념을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0018] 우선 순위 문제를 해결하기 위해서 멀티 팩터링(Multi-Factoring) 기술을 사용하는 멀티 액세스 액세스 제어라는 새로운 액세스 제어 메커니즘을 제안합니다.

[0019] 본 발명은 복수의 인증기관으로부터 권한을 획득할 수 있는 구성과, 속성으로 구성된 액세스 정책 트리의 구조를 동적으로 변경할 수 있고, 우선 순위가 높은 팩터(Factor)에 복잡한 보호 수준을 요구하며, 우선 순위가 낮은 팩터에 낮은 보호 수준을 설정할 수 있다.

[0020] 도 1은 본 발명의 실시예에 따른 우선 순위가 설정된 멀티 팩터 액세스 제어 시스템의 구성을 나타낸 도면이고, 본 발명의 실시예에 따른 액세스 정책 트리의 일례를 나타낸 도면이고, 도 3은 본 발명의 실시예에 따른 멀티 팩터 액세스 제어 시스템에서 인증 및 권한 부여 프로토콜의 액세스 제어 결정을 위한 프로토콜을 나타낸 도면이다.

[0021] 본 발명의 실시예에 따른 우선 순위가 설정된 멀티 팩터 액세스 제어 시스템(100)은 사용자 단말(110), 서비스 제공 단말(120) 및 인증기관(130)을 포함한다.

[0022] 사용자 단말(110)은 팩터(Factor)로 기능하는 팩터 키를 허가받은 인증기관(CA)(130)들에 연결한다. 팩터들은

팩터 키들(Secret Keys)을 의미한다.

[0023] 사용자 단말(110)은 복수의 인증기관(130)들로부터 복수의 팩터 키를 전송받는다. 여기서, 팩터 키는 일련의 속성으로 구성되며, 각 속성은 특정 액세스 조작에 대한 사용자 단말(110)의 특권을 나타낸다(예를 들어, 사무실 3803에 위치한 에어컨 제어 등).

[0024] 팩터 키 인가 프로세스는 사용자 단말(110)의 신원이 확인되고, 팩터 키가 포함된 속성들이 규정된다.

[0025] 복수의 인증기관(130)에서 팩터 키가 발급되기 때문에 하나의 팩터 키에 대한 타협은 다른 팩터 키에 영향을 미치지 않는다.

[0026] 사용자 단말(110)은 서비스 제공 단말(120)에 접근할 때 서비스 제공 단말(120)에 의해 준비된 보호 정책을 포함한 챌린지(Challenge)를 받게 된다.

[0027] 서비스 제공 단말(120)은 제시된 팩터 키들의 속성들에 따라 사용자 단말(110)을 인증한다.

[0028] 속성 기반 암호화(Attribute Based Encryption)는 공개 키를 사용하지 않고 속성 세트를 사용하여 데이터를 암호화한다.

[0029] 부울 수식은 액세스 정책 트리를 만들어 속성의 조합을 정의한다. 사용자 단말(110)은 액세스 정책 트리를 만족하는 경우 암호문을 해독할 수 있다.

[0030] 도 2에 도시된 바와 같이, 액세스 정책 트리는 두 가지 유형의 부울 로직 게이트와 나뭇잎에 있는 4가지 속성(Service Provider, Utility, EV, Read)으로 구성된다.

[0031] 액세스 정책 트리는 Service Provider와 Utility의 OR 게이트로 연결되고, EV와 Read의 AND 게이트로 연결되어 있으며, OR 게이트와 AND 게이트를 다시 AND 게이트로 연결되어 있다.

[0032] 일례로, 데이터 제공자(Alice)는 데이터를 암호화할 때 액세스 정책 트리를 생성하는데, Kevin과 Sara의 사용자 단말은 팩터 키들에 대한 5개의 속성들을 가진다.

[0033] 암호화 프로세스는 각각의 속성들을 논리 게이트로 매칭하여 True값이 모두 리턴되어야 데이터를 성공적으로 복구한다.

[0034] 즉, Service Provider 또는 Utility는 둘 중 하나의 속성이 True이어야 하고, EV와 Read는 두 가지의 속성이 모두 True이어야 한다.

[0035] 예를 들면, Kevin(Utility, Thermostat, EV, Read, Write), Sara(SP, Thermostat, Lighting, Heater, Read)인 경우, Kevin(사용자 단말)은 데이터 제공자(Alice)의 데이터를 읽는 반면, Sara(사용자 단말)은 데이터 제공자(Alice)의 데이터를 읽을 수 없다.

[0036] 서비스 제공 단말(120)은 액세스 정책 트리를 팩터 키들의 속성들을 이용하여 2개의 입력과 하나의 출력을 갖는 논리 회로를 복수로 구성된다.

[0037] 멀티 팩터 액세스 제어 시스템(100)은 트리의 부울 수식(Boolean Formula)을 동등한 선형 팩터 공유 스키마(Secret Sharing Schemes, LSSS) 행렬로 변환하여 수학적 형태로 정책을 나타낸다.

[0038] 분산된 액세스 제어 엔트리(Decentralized Access Control Entry, DeACE)는 세 가지의 사용자 클래스(소유자, 그룹 및 기타)를 미리 정의하고, 권한(읽기, 쓰기, 실행)이 각 클래스에 저장된다. 각 클래스의 권한은 사용자 단말(110)에게 읽기, 쓰기 또는 실행 권한이 부여되도록 3자리 코드로 표시된다. 즉, 사용자 단말(110)은 권한에 의해 "object_1=101" 권한을 부여받는다. 이를 해석하면, 사용자 단말(110)은 object_1에 액세스하면, 읽기 및 실행 권한이 있지만 쓰기 권한이 없다.사용자 단말(110)은 다른 인증기관(130)에 의해 부여된 복수의 속성 세트들을 저장한다.

[0039] 액세스하는 사용자 단말(110)은 데이터를 복구하기 위해 적절한 속성 세트를 제시해야 하며, 2개의 인증기관(130)에서 부여된 속성을 독립적으로 확보해야 한다.

[0040] 각각의 인증기관(130)은 다양한 형태의 속성들의 집합을 저장하고 있다.

[0041] 속성 형태는 조명, 에어컨, 팬, 태양광 패널과 같은 스마트 빌딩 내의 에너지 소스들을 나타내고, 회사의 특정 직원(예를 들어 직원 ID 및 이름)을 포함한다.

[0042] 멀티 팩터 액세스 제어 시스템(100)은 새로운 형태의 속성인 클리어런스(Clearance)를 추가한다. 클리어런스의 카테고리는 매니저, 관리자, 번호가 할당된 구성원이 포함된다.

[0043] 클리어런스의 번호는 속성 내의 클리어런스 레벨을 나타낸다(예를 들면, "manager = 300").

[0044] 사용자 단말(110)은 인증기관(130)에 접속하여 팩터 키를 수신한다. 사용자 단말(110)은 복수의 인증기관(130)과 통신망(102)을 통해 통신하여 복수의 팩터 키들과 팩터 키의 집합을 전송받는다.

[0045] 사용자 단말(110)은 액세스 요청 메시지를 생성하여 통신망(102)을 통해 서비스 제공 단말(120)로 전송한다.

[0046] 서비스 제공 단말(120)은 사용자 단말(110)로부터 액세스 요청 메시지를 수신하면, 하나 또는 하나 이상의 팩터 키를 사용자 단말(110)로 제공한다.

[0047] 서비스 제공 단말(120)은 액세스 요청을 처리하기 위해서 액세스 정책 트리(도 2), 챌린지(Challenge)를 유지 관리한다.

[0048] 액세스 정책 트리의 속성들은 하나의 인증기관(130)에 속할 수도 있고, 각 속성들이 다른 인증기관(130)에 속할 수도 있다.

[0049] 예를 들면, 도 2에 도시된 바와 같이, 앨리스(Alice)는 캘리포니아주에서 발행한 두 가지 속성(서비스 제공업체 및 유틸리티)과 로스앤젤레스시에서 발행한 두 가지 속성(전기 자동차 및 읽기)을 사용할 수 있다.

[0050] 팩터 키들의 개수는 보호 레벨을 결정한다. 번호로 지정된 속성의 경우, 서비스 제공 단말(120)은 "manager = 200"과 같은 부등호를 사용하여 클리어런스 레벨에 대한 조건을 설정한다.

[0051] 사용자 단말(110)은 챌린지를 만족시키는 팩터 키와 속성들을 제시하면, 액세스 요청이 확인되고 수락된다.

[0052] 서비스 제공 단말(120)은 팩터 키들의 개수를 변경하여 다양한 챌린지를 동적으로 생성할 수 있고, 응용 프로그램의 컨텍스트에 따라 속성 조합을 생성할 수 있다.

[0053] 멀티 팩터 액세스 제어 시스템(100)은 공공 매개변수인 P_{aram}을 모든 인증기관(130)들과 사용자 단말(110)로 전송한다. 여기서. P_{aram}은 하기의 [수학식 1]과 같이 정의된다.

[0054] 바이리니어 맵(Bilinear Map) e가 정의된 3개의 그룹 G_1, G_2, G_T들을 고려하는 경우, 상기 그룹 G_1, G_2는 수학적으로 정의되는 위수(Order)가 큰 소수(Prime Number)인 싸이클릭 그룹들이다.

[0055] 싸이클릭 그룹은 하나의 원소로 생성될 수 있는 그룹을 의미하므로 두 그룹의 생성원을 고정하여 사용하는데, 제1 싸이클릭 그룹 G_1 생성원을 g1, 제2 싸이클릭 그룹 G_2의 생성원을 g2로 표기하기로 한다. 이때, 다음의 사상을 만족하는 상기 바이리니어 맵(Bilinear Map) $e : G_1 \times G_2 \rightarrow G_T$이 있다고 가정한다.

수학식 1

[0056] $$\mathcal{P}_{aram} = \langle g, H \rangle$$

[0057] 여기서, g는 그룹 G의 생성기(Generator), 해시 함수(Hash Function) $H : \{0,1\}^* \rightarrow G$는 사용자 단말(110)의 인증을 위해 G를 매핑한다.

[0058] 인증기관(CA_j)(130)은 속성 세트 L_j를 유지 관리한다.

[0059] 인증기관(CA_j)(130)은 각각의 속성 $i \in L_j$에 대해서 두 개의 임의의 지수 $\alpha_i, y_i \in \mathbb{Z}_N$를 선택하고, 팩터 키와 공개 키의 2가지 Key를 생성한다. 인증기관(130)은 하기의 [수학식 2]에 의해 팩터 키 SK_j를 유지하고, 공개 키 PK_j를 생성한다.

수학식 2

[0060] $$SK_j = \{\alpha_i, y_i | \forall i\}, PK_j = \{e(g,g)^{\alpha_i}, g^{y_i} | \forall i\}$$

[0061] 팩터 키 SK_j와 공개 키 PK_j는 인증기관(CA_j)(130)에서 생성되어 사용자 단말(110)과 서비스 제공 단말(120)로 전송된다.

[0062] 인증기관(130)은 인증 요청에 따라 사용자 단말(110)의 신원을 검증한다. 인증기관(130)은 사용자 단말(110)에 대한 정규화된 속성 집합($L_{j,u} \subset L_j$)을 선택하고, [수학식 3]에 의해 속성 집합에 대응하는 팩터 키 세트를 생성한다.

수학식 3

[0063] $$FK_{j,u} = \{K_{i,u} = g^{\alpha_i} H(u)^{y_i} | \forall i \in L_{j,u}\}$$

[0064] 여기서, H(u)는 사용자 단말(110)의 ID의 해시이고, $FK_{j,u}$는 팩터 키 $\mathcal{F}_{j,u}$가 포함된 팩터 키 집합이다. 팩터 키 세트 $\mathcal{F}_{j,u}$는 인증기관(CA_j)(130)이 사용자 단말(110)에 부여하는 것이고, 일련의 속성 집합과 대응하는 팩터 키들을 포함한다.

[0065] 그런 다음, 인증기관(CA_j)(130)은 팩터 키 $\mathcal{F}_{j,u}$를 사용자 단말(110)에게 발급해준다. 이를 하기의 [수학식 4]와 같이 표현된다.

수학식 4

[0066] $$CA_j \mapsto u : \mathcal{F}_{j,u} = \langle L_{j,u}, FK_{j,u} \rangle$$

[0067] 여기서, $L_{j,u}$는 팩터 키 $\mathcal{F}_{j,u}$가 포함된 속성 집합이고, $FK_{j,u}$는 팩터 키 $\mathcal{F}_{j,u}$가 포함된 팩터 키들의 집합을 나타낸다.

[0068] 예를 들면, 도 2에 도시된 바와 같이, 사용자 단말(110)은 인증기관(130)으로부터 서비스 프로바이더(Service Provider), 유틸리티(Utility), EV, Read의 4가지 속성이 포함된 팩터 키 세트를 제공받는다.

[0069] 사용자 단말(110)은 서비스 제공 단말($\tilde{u}$)(120) 상에서 특정 작업을 수행하기 위하여 서비스 제공 단말($\tilde{u}$)(120)을 액세스한다.

[0070] 예를 들면, 서비스 제공 단말(120)이 히터라고 가정하면, 사용자 단말(110)은 히터를 오프하라는 액세스 요청 메시지(Mo)를 생성하여 히터인 서비스 제공 단말(120)로 전송하고, 본인을 나타내는 랜덤번호인 $\hat{a} \in \mathbb{Z}_q$를 생성한다. 사용자 단말(110)은 액세스 요청(Access Request, AR) 메시지를 생성하여 서비스 제공 단말(120)로 전송한다. 여기서, 액세스 요청 메시지는 다음의 [수학식 5]와 같다.

수학식 5

[0071] $$u \mapsto \tilde{u} : \mathcal{AR} = \langle g^{\hat{a}}, M_o \rangle$$

[0072] 서비스 제공 단말($\tilde{u}$)(120)은 사용자 단말(110)로부터 액세스 요청 메시지를 수신하는 경우, 사용자 단말(110)을 인증하는데 사용되는 챌린지(Challenge)를 생성한다.

[0073] 예를 들면, $u \mapsto \tilde{u} : M$, 사용자 단말(110)은 메시지 M을 서비스 제공 단말(120)로 전송한다는 의미이다.

[0074] 서비스 제공 단말($\tilde{u}$)(120)은 2개의 랜덤번호인 $\hat{b}$ and $\hat{c} \in \mathbb{Z}$ 를 생성하고, 시퀀스 번호 z를 생성한다.

[0075] 서비스 제공 단말($\tilde{u}$)(120)은 랜덤번호인 $\hat{b}$ and $\hat{c} \in \mathbb{Z}$, 시퀀스 번호 z와, 액세스 요청 메시지에서 획득한 $g^{\hat{a}}$ 를 이용하여 2개의 변수($z_1 = g^{\hat{b}}$ and $z_2 = enc_z(\hat{c}, (g^{\hat{a}})^{\hat{b}\hat{c}})$)를 계산한다.

[0076] 여기서, $enc_x(y)$ 는 메시지 y를 팩터 x로 암호화하는 대칭 키 알고리즘이고, 암호 해독에 대한 쌍 표기법은 $y=dec_x(ciphertext)$이다.

[0077] 서비스 제공 단말($\tilde{u}$)(120)은 전술한 2개의 변수를 연결하여 챌린지 메시지(Mc)를 생성한다. 예를 들면, $\langle M_1, M_2 \rangle$ 는 메시지 M1와 M2를 연결한다는 의미이다.

수학식 6

[0078] $$M_c = \langle z_1, z_2 \rangle$$

[0079] 서비스 제공 단말($\tilde{u}$)(120)은 도 2와 같이, 액세스 정책 트리 $\mathcal{T}$ 를 생성하여 보호 정책을 구축한다. $\mathcal{T}$ 는 서비스 제공 단말(120)을 구축하는 액세스 정책 트리이고, 서비스 제공 단말(120) 상에서 액세스 조작의 보호 레벨을 나타낸다. 여기서, 도 2는 액세스 정책 트리의 일례를 나타낸다.

[0080] 서비스 제공 단말(120)은 인증기관(130)의 공개 키 PK로부터 액세스 정책 트리의 모든 속성들에 관련된 팩터들과 팩터 키들을 획득한다.

[0081] 서비스 제공 단말(120)은 액세스 정책 트리를 등가의 n×l의 LSSS(Linear Secret Sharing Scheme) 매트릭스($\mathcal{A}$)로 변환한다. 여기서, $\mathcal{A}$ 는 $\mathcal{T}$ 에 대응하는 LSSS 매트릭스이고, n은 액세스 정책 트리의 형태를 결정하고, l은 액세스 정책 트리의 속성 개수이다.

[0082] 액세스 정책 트리를 LSSS 매트릭스로 변환하는 일례는 다음과 같다.

Algorithm: LW vector space construction

```
   input  : access policy tree T
   output : a LSSS matrix A
1  assign a vector (1) (of length of 1) to root node
2  traverse down the tree from root to leaves
     set v = vector at current node n;
     set c = length of v;
5    if (OR gate) // assign same vector v to children
         set vc = v;
7    else if (AND gate)
         if (left child) // concatenate a vector (1) to v
             set vc = v | 1;
         else // concatenate a vector (-1) to zero vector
             set vc = (0,…,0) | -1
         endif
         set c = c + 1;
14   endif
15 end of traverse
```

Access policy tree

$\mathcal{T}$ = { A AND (D OR (B AND C)) }

↕

A LSSS matrix $\mathcal{A}$

$$\begin{array}{c} \\ A \\ B \\ C \\ D \end{array}\begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

[0083]

[0084] 전술한 알고리즘은 액세스 정책 트리(도 2)를 텍스트 형태를 매트릭스 형태로 변환한 것이다.

[0085] 서비스 제공 단말(120)은 챌린지 메시지(Mc), 공개 키(PK), LSSS 행렬($\mathcal{A}$)을 계산한 후, 아래의 변수들을 계산할 수 있다.

[0086] 서비스 제공 단말(120)은 속성의 전체를 나타내는 랜덤번호인 $s \in \mathbb{Z}_N$ 벡터를 생성하고, 제1 엔트리로 S를 가진 $v \in \mathbb{Z}_N^l$ 벡터와 제1 엔트리로 0을 가진 $w \in \mathbb{Z}_N^l$ 벡터의 2개의 랜덤 벡터를 생성한다.

[0087] 서비스 제공 단말(120)은 $\lambda_x = \mathcal{A}_x \cdot v \text{ and } w_x = \mathcal{A}_x \cdot w$ 를 계산한다. 여기서, $\mathcal{A}_x$는 $\mathcal{A}$ 의 행 X이다.

[0088] 서비스 제공 단말(120)은 $\mathcal{A}$ 의 각 행 $\mathcal{A}_x$에 대하여 랜덤번호인 $r_x \in \mathbb{Z}_N$ 을 생성한다. 즉, r_x는 속성별 랜덤번호를 나타낸다.

[0089] 서비스 제공 단말(120)은 인증기관(130)로부터 액세스 정책 트리($\mathcal{T}$)의 각 속성(i)별 위치를 나타내는 $\rho(x)$ 를 획득한다.

[0090] 서비스 제공 단말(120)은 하기의 [수학식 7]과 같이, 바이리니어 맵(Bilinear Map)의 S자승에 Mc를 곱하면 ($Mc(e(g,g)^S$), 검증할 데이터를 포함한 Co가 계산된다.

[0091] 서비스 제공 단말(120)은 행렬 $\mathcal{A}$ 와 ρ, Co, $C_{1,x}$, $C_{2,x}$, $C_{3,x}$를 모두 연결하여 챌린지(C)를 생성하고, 생성된 챌린지(C)를 사용자 단말(110)로 전송한다. 여기서, 챌린지(C)는 다음의 [수학식 7]과 같다.

수학식 7

[0092]
$$\mathcal{C} = \langle \mathcal{A}, \rho, C_0 = M_c e(g,g)^s$$
$$C_{1,x} = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\rho(x)} r_x} \forall x$$
$$C_{2,x} = g^{r_x} \forall x, C_{3,x} = g^{y_{\rho(x)} r_x} g^{w_x} \forall x \rangle$$
$$\tilde{u} \mapsto u : \mathcal{C}$$

[0093] Co, $C_{1,x}$, $C_{2,x}$, $C_{3,x}$는 속성을 나타내고, C1,x는 바이리니어 맵(Bilinear Map)(e(g,g))의 λ_x 자승과, 바이리니어 맵(e(g,g))의 $\alpha_{\rho(x)} r_x$ 자승으로 암호화한다.

[0094] 챌린지(C)는 액세스 정책 트리(도 2)를 나타내는 텍스트 형태를 매트릭스 형태로 변환하고, 매트릭스 형태를 수학적으로 암호화한 것이다(수학식 7).

[0095] 챌린지(C)는 사용자 단말(110)이 갖고 있는 속성(Co, C_1, C_2, C_3)으로 트리 구조를 만들어 암호화한다.

[0096] 사용자 단말(110)은 서비스 제공 단말(120)로부터 챌린지(C)를 수신하는 경우, 행렬 $\mathcal{A}$와 ρ를 획득한다.

[0097] 팩터 키 집합 $\mathcal{F}_u$은 속성 집합 $\{\rho(x) : x \in \mathcal{A}_x\}$에 대한 $K_{\rho(x),u}$에 상응하는 팩터 키들을 포함한다면, 사용자 단말(110)은 다음 단계를 진행한다. 그렇지 않은 경우, 사용자 단말(110)은 자격이 없으므로 프로세스를 중단한다.

[0098] 사용자 단말(110)은 n개의 복수의 인증기관(130)에서 부여된 팩터 키의 집합, 즉 $\mathcal{F}_u = \{\mathcal{F}_{1,u}, \ldots, \mathcal{F}_{n,u}\}$를 유지한다.

[0099] 챌린지(C)와 팩터 키들로부터 다른 변수들을 얻는 경우, 사용자 단말(110)은 [수학식 8]에 의해 각 x를 계산할 수 있다.

수학식 8

[0100]
$$val(x) = \frac{C_{1,x} \cdot e(H(u), C_{3,x})}{e(K_{\rho(x),u}, C_{2,x})}$$
$$\prod_x (val(x))^{c_x} = \prod_x (e(g,g)^{\lambda_x} e(H(u),g)^{w_x})^{c_x} = e(g,g)^s$$

[0101] 사용자 단말(110)은 $\sum_x c_x \mathcal{A}_x = (1, 0, \ldots, 0)$이 되도록 상수 $c_x \in \mathbb{Z}_N$를 선택하고, 하기의 [수학식 9]에 의해 미래 평가를 위한 챌린지 메시지 신호 M_c'를 복구한다.

수학식 9

$$M_c' = \frac{C_0}{e(g,g)^s} = \langle z_1', z_2' \rangle$$

[0102]

[0103] 사용자 단말(110)은 액세스 요청 절차에서 미리 선택된 랜덤번호 $\hat{a} \in \mathbb{Z}$를 이용하여 챌린지 응답 신호(CR)를 생성하고, 생성한 챌린지 응답 신호를 서비스 제공 단말(120)로 전송한다(수학식 10).

수학식 10

$$u \mapsto \tilde{u} : \mathcal{CR} = \langle (z_1')^{\hat{a}'}, z_2' \rangle$$

[0104]

[0105] 여기서, $\hat{a}'$는 미래 평가에 있어 $\hat{a}$ 대신에 사용된다.

[0106] 서비스 제공 단말(120)은 사용자 단말(110)로부터 챌린지 응답 신호를 수신하는 경우, z_2'를 획득하고, 챌린지 생성 절차에서 사용된 고유 시퀀스 번호 Z를 사용하여 $dec_z(z_2') = \langle \hat{c}, (g^{\hat{a}})^{\hat{b}\hat{c}} \rangle$의 복호화 연산 과정을 계산할 수 있다.

[0107] 그런 다음, 서비스 제공 단말(120)은 하기의 [수학식 11]과 같이 2개의 변수를 비교한 후, 비교 결과가 동일하면, True를 반환하면, 요청된 연산자 Mo를 수행하고, Ack 신호를 생성하여 사용자 단말(110)로 전송한다. 비교 결과가 동일하지 않으면, 서비스 제공 단말(120)은 액세스 요청을 거부한다. 예를 들면, 서비스 제공 단말(120)은 True인 경우, 액세스 요청 메시지(Mo)에 따라 히터를 오프시키고, False인 경우, 히터를 오프시키지 않고 액세스 요청을 거부한다.

수학식 11

$$((z_1')^{\hat{a}'})^{\hat{c}} = (g^{\hat{a}})^{\hat{b}\hat{c}}$$

[0108]

[0110] 도 4는 본 발명의 실시예에 따른 스마트 그리드의 멀티 팩터 액세스 제어를 사용하여 에너지 자원에 대한 세분화된 액세스 제어 개념을 나타낸 도면이다.

[0111] 본 발명의 멀티 팩터 액세스 제어 시스템(100)은 에너지 자원(120)을 제어하는 데이터 리딩 및 제어의 액세스 작업을 위하여 보호 수준의 난이도를 차별화한다.

[0112] 제1 사용자 단말(111)은 데이터 리딩(Reading)의 액세스 작업을 위하여 하나의 인증기관(130)에 권한을 부여받는다.

[0113] 제2 사용자 단말(112)은 제어(Control)의 액세스 작업을 위하여 2개의 인증기관(130)에 권한을 획득해야 한다.

[0114] 본 발명은 에너지 자원(120)을 제어하는 두 가지 유형으로 데이터 리딩과 제어의 팩터(Factor)를 제공한다.

[0115] 본 발명의 멀티 팩터 액세스 제어 시스템(100)은 도 2와 같이, 속성으로 구성된 액세스 정책 트리를 생성하고,

일정 시 간 후에 액세스 정책 트리의 구조를 동적으로 변경할 수 있으며, 보호 수준의 난이도를 다르게 설정할 수 있다.

[0116] 본 발명은 복수의 인증기관(130)으로부터 권한을 획득할 수 있는 구성, 속성별로 팩터 키가 존재하는 구성, 속성으로 구성된 액세스 정책 트리의 구조를 동적으로 변경할 수 있고, 우선 순위가 높은 팩터(Factor)에 복잡한 보호 수준을 요구하며, 우선 순위가 낮은 팩터에 낮은 보호 수준을 설정할 수 있다.

[0117] 이상에서 본 발명의 실시예는 장치 및/또는 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하기 위한 프로그램, 그 프로그램이 기록된 기록 매체 등을 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

[0118] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

부호의 설명

[0119] 100: 멀티 팩터 액세스 제어 시스템

102: 통신망

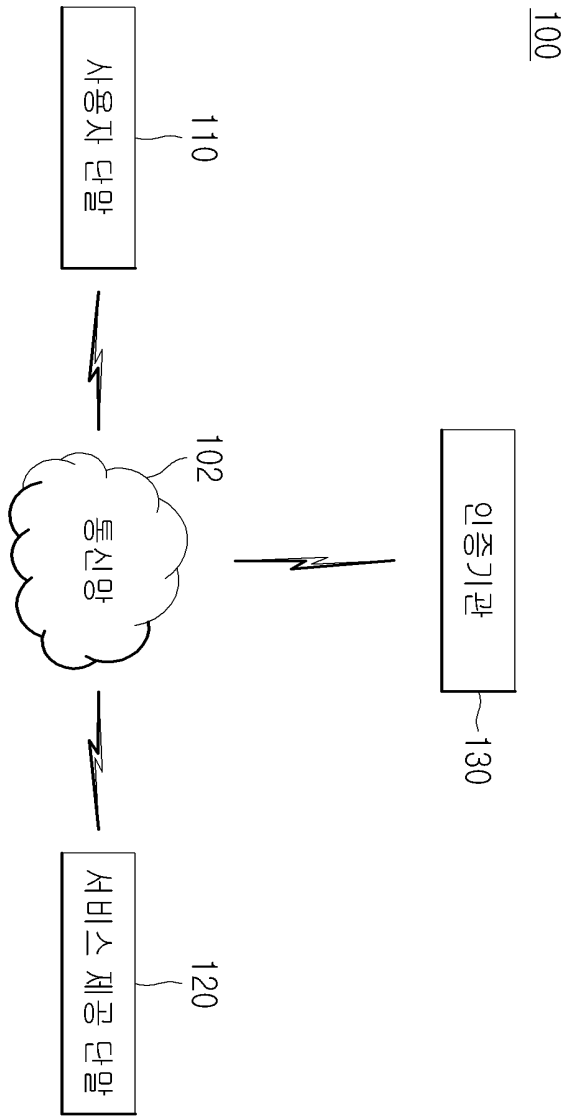
110: 사용자 단말

120: 서비스 제공 단말

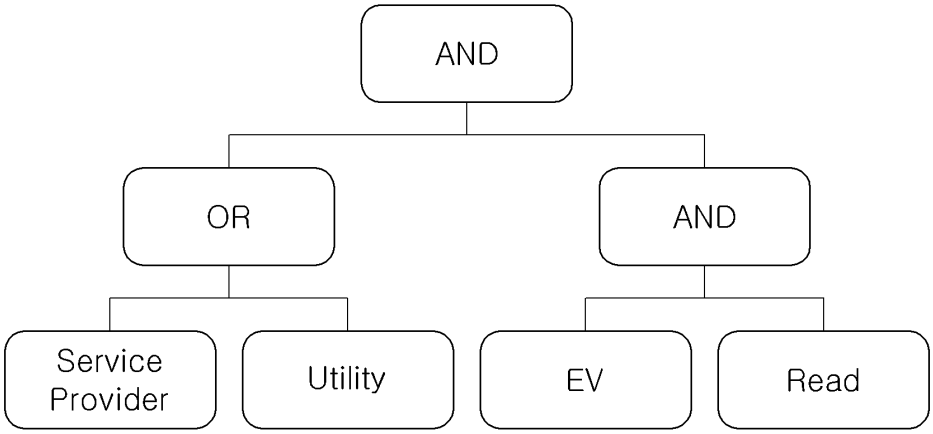
130: 인증기관

도면

도면1

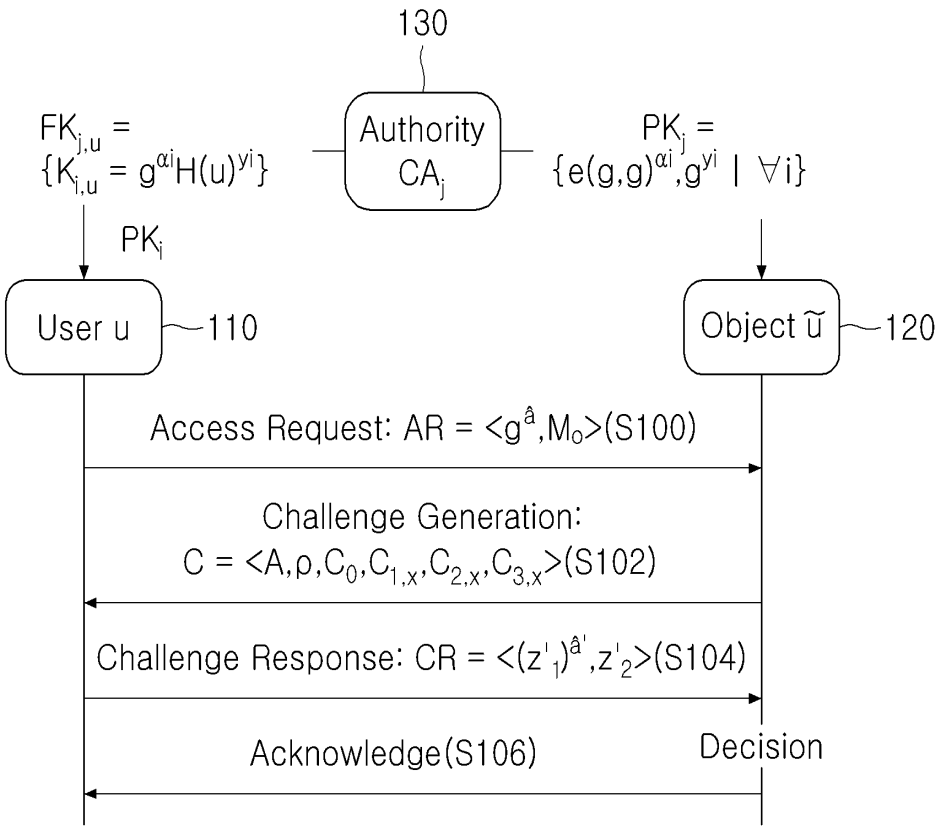


도면2

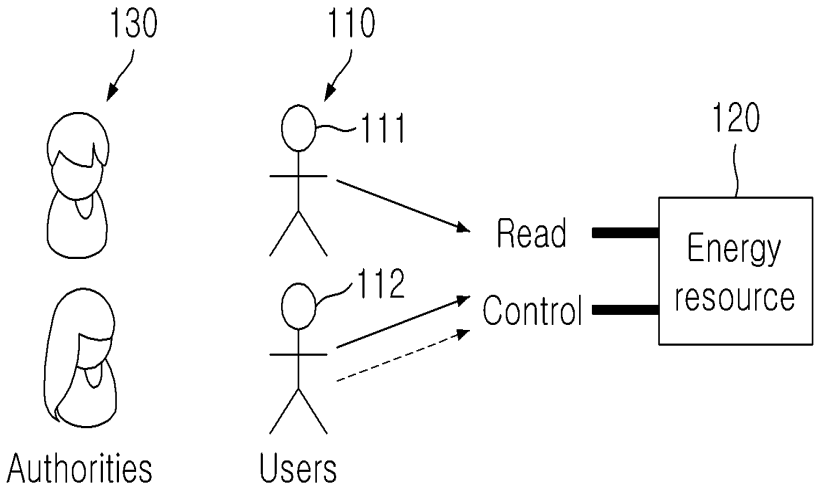


*Kevin, {Utility, Thermostat, EV, Read, Write
*Sara, {SP, Thermostat, Lighting, Heater, Read}

도면3



도면4


130
110
111
120
Read
Energy
resource
112
Control
Authorities
Users